Integrating Domain Name Services on the State of Missouri
Private Backbone
(Approved by ITAB, January 27, 1999)

Summary:

Agencies will be setting up services (web servers, gateways, etc.) using the state's private TCP/IP backbone. These services could then be available, as appropriate, to other state agencies but not necessarily to anyone on the public Internet). In order to achieve this capability, the following items must be established:

- *A consistent, structured naming standard for these services*
- *A mechanism to enable **location** of these services via the structured naming standard (i.e., domain name servers)*
- *Procedures to ensure that security for non-shared resources is maintained*
- *Agency connection to the state's private TCP/IP backbone, if necessary*
- *Agency migration, if necessary, to the 10.x.x.x ~ TCP/IP structure*

The driving forces toward this capability include both TCP/IP gateways into the mainframe and server based gateways for the MAIRS and SAM II projects, as well as access to the web-based SAM II data warehouse. In the near future, we also see the need for agencies to setup intranet (i.e., inside the state's private network structure) servers for access by different agencies within state government. An example would be a web server set up by the Department of Social Services (DSS). DSS could provide information on a multi-agency children's initiative to staff from partner agencies such as the Department of Mental Health or the Governor's Office.

The first requirement, the consistent naming structure, has been established. The TCP/IP domain "state.mo.us" has been established for both external (Internet) and internal (intranet) services. The domain has then been divided into agency subsets of the naming structure. Examples of this include:

oa.state.rno.us
dnr.state.mo.us
dmh.state.rno.us

For ease of workstation configuration, a common subset (intra.state.mo.us) has also been established. This allows common configuration of personal computers throughout state government for commonly accessed services (e.g., MAIRS, SAM 11) available via the state's private TCP/IP backbone.

In order to complete the requirements for this private network structure, the following steps will be necessary:

- *A private root domain name server for the state.mo.us and other state government domains will be identified.*

- *Other private* name *servers would be designated as name servers for sub domains of the state.mo.us domain.*
- *Integration of the multiple private domain name servers maintained by state agencies must be accomplished.*

Technical Background

The State of Missouri public (i.e. **non-Secure)** TCP/IP backbone connects to **the** Internet via MOREnet. State agencies connect their LANs to the public backbone to obtain access to the Internet and to interconnect with the LANs of other agencies. Since the public TCP/IP backbone does directly connects to the Internet and cannot be considered secure, the agency connections to that backbone should be mediated by a firewall. Most agencies not choosing to maintain their own firewall are connected through a shared firewall operated by the State Data Center (SDC).

In addition to interagency connectivity via the public backbone many state agencies are also connecting to a private TCP/IP backbone. Policy requires that all agencies connecting to both the public and private backbones must use an approved firewall to mediate the connection between the agency LAN and the public backbone. The agencies can also use another firewall, filtering router, or other means to isolate the confidential resources on their LAN from the state's private TCP/IP backbone.

Properly configured firewalls require separate domain name servers (DNS) for the protected and the public network. Public DNS is the services.state.mo.us server. This server is the authoritative Internet DNS for the state.mo.us domain. Each of the several firewalls connected to the state's public backbone also have private domain name services. Some agency servers, internal mail servers for instance, will be defined on the agencies private DNS only. Although all agencies access the public DNS only the owning agency has access to the private DNS.

Private Root Name Server

The domain name server **dogwood.state.mo.us has** been designated the primary name server for state.rno.us and some other state government domains. Its secondary name server is pinnacle.state.mo.us. The other state domain's carried on dogwood are:

- apwaism.org
- aphsa-ism.org
- mdfb.org
- missouritourisrn.org
- missouriartscouncil.org
- womenscouncil.org

Agency Private Name Servers
The various agencies may choose to support a private name server within their private TCP/IP structure. The domain name being supported will normally be a sub domain of the "state.mo.us" structure. Examples of private sub domains supported by a name server within the agencies would include:

dolir.state.mo.us
dmh.state.mo.us

Name resolution from the root name server perspective
The root name server will be responsible for name resolution of all *.state.mo.us hosts, and can either control entire sub domains (e.g., oa.state.mo.us), or delegate authority for a sub domain (e.g., dnr.state.mo.us) to a specific agency's private name server. When end-users define the private root name server (dogwood) as their primary DNS server, the root server can then resolve the address, delegate a request to a private agency DNS, or forward the request out the state's firewall.

As requested, new agency-registered domains will be added to dogwood. For example, the State Treasurer's office would ask that the domain "treasurer.state.mo.us" be defined at the root name server, and the host www.treasurer.state.mo.us be defined as a host within the domain.

Name resolution from an private agency name server perspective Each agency operating a private domain name server (e.g., dnr.state.mo.us) would configure that server as a secondary name server for the domains defined on dogwood, or use a forwarder to dogwood to resolve the intranet addresses.

The agencies have two options for the "forwarders" statement of their private domain name server configurations:

- Use dogwood.state.mo.us as the forwarder
- Set up the local name server as secondary for all state domains and set the forwarders statement of the local name server to the agency firewall

Agency Intranet Server Requirements
Agencies wishing to have intranet servers defined (for access l:y other state agencies) have two options for narning the service:

1) Register the server in the intra.state.mo.us sub domain. For example, the SAM U data warehouse could be known as **sam2dwh.intra.state.mo.us.** Systems such as SAM II, MAIRS, and others accessible by all agencies via a private network TCP/IP connection would fall under this naming scheme. From a browser standpoint, this would allow agencies to configure their end-user devices to exclude any *.intra.state.mo.us hosts from using a proxy or Socks connection (forcing the connection over the state's private network structure). Using the wildcard eases the burden of having to configure exclusions for each host that would be accessible via the state's intranet, as long as they fell under the

*.intra.state.mo.us naming convention.

2) Agencies using a delegated sub domain of state.mo.us (e.g., health.state.mo.us) would request an alias entry at the primary root name server for SOMETHING.intra~state.mo.us to make an intranet server addressable to other agencies. If the Department of Health, for example, wanted to give intranet access to other agencies to it's private server known as **dohwww.hcalth.state.mo.us,** it could register an alias, such as **dohwww.intra.state.mo.us,** for the system. The other agencies would then use this URL when accessing the Health server.

Security Responsibilities

Agencies allowing access to internal servers must ensure that the link between their agency LAN and the state's private TCP/IP backbone is sufficiently secured, either by filtering router or by a firewall, if the agency requires such security.

The state's private root name server (dogwood) should not be secondary to any agency's private name server. This could expose names and correlating IP addresses within the agency to scrutiny outside the agency within the state's private network. It could also create an unnecessary amount of overhead on the state's root and secondary name servers.

10 Dot addressing issues

The migration to 10. * (and other REC 1918) addressing should be accelerated on the state's private backbone. This will ease the issue of continuing agency router configuration changes. The use of the 168.166.x.x addressing scheme should be discontinued, or at least offer a secondary addressing scheme for these hosts that follow the 10.* address format.